UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF NEBRASKA

PRISM TECHNOLOGIES, LLC,

Plaintiff,

v.

ADOBE SYSTEMS INCORPORATED; AUTODESK, INC.; MCAFEE, INC.; NATIONAL INSTRUMENTS CORPORATION; NUANCE COMMUNICATIONS, INC.; QUARK, INC.; THE SAGE GROUP PLC; SAGE SOFTWARE INC.; SYMANTEC CORPORATION; THE MATHWORKS, INC.; and TREND MICRO INCORPORATED,

Defendants.

Civil Action No. 8:10-cv-00220-LES-TDT

DEFENDANTS' OPENING CLAIM CONSTRUCTION BRIEF REGARDING "HARDWARE KEY" AND "ACCESS KEY"

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

I. INTRODUCTION

The patent-in-suit, U.S. Patent No. 7,290,288 (the "'288 patent") (Ex. A), is directed to a secure network transaction system that uses external hardware keys to provide added protection over traditional usernames and passwords. The hardware key (also known as an "access key") is encoded with a unique digital identification that is assigned to a specific account holder. That digital identification is read from the hardware key when it is connected to the account holder's computer, and compared with the digital identification stored at an authorization server to authenticate the account holder and provide access to the secure transaction system.

All claims of the '288 patent require either a "hardware key" or "access key." The District Court for the District of Delaware previously construed "hardware key" to mean **"an external hardware device or object from which *the predetermined* digital identification can be *read*,"** and acknowledged Prism's agreement that "hardware key" and "access key" mean the same thing. Prism did not appeal that construction.

All ten Defendants in this case believe that the Delaware court's construction of these terms was proper in every respect, and urge this Court adopt it verbatim. Prism, on the other hand, now proposes that this Court reject the Delaware court's construction, and construe "hardware key" and "access key" to mean an **"external hardware device or object from which *a* digital identification can be *generated, derived or* read."** By broadening not only *what kind* of digital identification is read from the hardware key, but *whether* that digital identification must be read from the hardware key at all, Prism seeks to eliminate the major purpose of the hardware key – to uniquely identify a user. Accordingly, two disputes are presented here: whether this Court should broaden the Delaware court's construction by (1) no longer requiring the digital identification to be "read" from the hardware key, and/or (2) no longer requiring what *is* read to be "the predetermined digital identification." Both proposed changes are improper, unsupported by the patent's written description, and inconsistent with the Delaware court's opinion and Prism's own previous statements.

The Court should adopt the Delaware court's construction as-is because, unlike Prism's proposed construction, it stays true to the claim language and most naturally aligns with the patent's description of the invention. The patent says the major purpose of the hardware key is to "uniquely identify an account holder." It discloses several embodiments of a hardware key, and in every one, the digital identification is stored on, and read from, the hardware key. Further, in every embodiment, the digital identification is predetermined so it can be used by the server for two-factor authentication.

Prism's proposed construction is crafted to circumvent the hardware key requirement. Defendants design and develop a variety of different kinds of software that can be installed on end users' computers. None of the Defendants use any kind of external hardware key for authentication. In some cases Defendants provide users with external software installation CDs. Even where an installation CD is used, however, it is an exact duplicate of an original master CD and does not store any kind of unique digital identification to identify a user – in other words, it is by no stretch a "hardware key." After Defendants' software is installed on a user's computer, it may in some instances require activation to prevent unauthorized copying of the software; but in no instance does activation involve reading any kind of unique digital identification from the CD or otherwise using that CD to uniquely identify a user.

Since Prism's proposed construction is at odds with the specification, the file history, the claims, the Delaware construction, and statements made by Prism in prior litigation, it should be rejected. This Court should construe both "hardware key" and "access key" as "***an external hardware device or object from which the predetermined digital identification can be read***."

II. TECHNICAL BACKGROUND

Although only the ’288 patent is asserted against Defendants in this case, there are two Prism patents relevant to claim construction – the ’288 patent, and Prism’s earlier patent, U.S. Patent No. 6,516,416 (the “’416 patent”) (Ex. B). Prism contends that the ’288 patent is a “continuation-in-part” of the ’416 patent, meaning both patents originated, at least in part, from the same patent application and written description.[1] In patent parlance, the originally filed ’416 patent is the “parent” patent, and the asserted ’288 patent is the “child” patent. The specification of a parent patent is generally relevant to construction of a child patent. *See Microsoft Corp. v. Multi-Tech Sys.,* 357 F.3d 1340, 1349-50 (Fed. Cir. 2004). This is particularly so here, because the term “access key” – found in the ’288 patent claims – does not appear anywhere in the ’288 specification, but is present in the ’416 parent specification, where it is used interchangeably with the term “hardware key.” (*See, e.g.*, Ex. B at 7:59-65.)

A. The ’416 Patent

The ’416 patent was filed on June 11, 1997, at a time when content providers like America Online (“AOL”) made their proprietary content available over the Internet using a monthly subscription model. These content providers wanted to make some information available to the general public for free, but wanted to keep other content restricted to only their paying customers. The ’416 patent notes that “information providers may provide information without charge for certain information that can be accessed by any user that has access to the network. However, the same information providers may want to generate revenue from subscription service and also to protect its information assets.” (Ex. B at 1:8-27.) The ’416 patent goes on to explain that traditional authentication using a username and password is

[1] The parties dispute whether Prism is entitled to claim the benefit of the 1997 filing date of the ’416 patent instead of the 2002 filing date of the ’288 patent-in-suit. That dispute, however, is not immediately relevant to the issues presented here.

inadequate because subscribers can share usernames and passwords with friends (or post them on Internet newsgroups), allowing unauthorized individuals to access protected content for free. (*Id*. at 1:28-46.)

B. The ’288 Patent

The ’288 patent was filed on August 29, 2002, five years after the ’416 patent was filed. By that time, the subscription model described in the ’416 patent was becoming obsolete, and the focus of the Internet community had shifted to online business. Prism rewrote portions of the ’416 patent specification to reflect a focus on e-commerce – replacing “subscription access system” with “secure transaction system” – and describing the invention as “providing a platform for securing transactions between consumers and suppliers on an untrusted network.” (Ex. A at 3:44-46.) The problem of restricting access to only authorized users remained the same: “Such businesses may provide transaction services without charge for certain transactions that can be accessed by any account holder having access to the network. However, the same business may want to generate revenue from other transaction services and also to protect its business assets.” (*Id*. at 1:13-25.) The ’288 patent, like the ’416 patent, notes the inadequacy of traditional username/password authentication: “Such schemes are vulnerable to password fraud because account holders can share their usernames and passwords by word of mouth or through Internet news groups, which obviously is conducive to fraudulent access and loss of revenue.” (*Id*. at 1:31-35.)

C. Two-Factor Authentication

To solve this alleged problem, both the ’288 and ’416 patents use “two factor authentication” to protect restricted content. (*See* Ex. A at 5:37-45; Ex. B at 7:59-65.) Two-factor authentication was well-known at the time these patents were filed and, as its name implies, uses two different pieces of data to authenticate a user. That typically means combining something the user knows as a secret (e.g., a password or personal identification number) with something the user uniquely has in his or her physical possession (e.g., an access card with a unique digital identifier that only the user possesses). A familiar example of two-factor identification is a bank ATM card: a bank user must *physically possess* an ATM card, which has a unique digital identifier embedded on a magnetic strip (e.g., the user's name and account number), and the user must *know* the secret PIN associated with that account in order to withdraw money.

In the case of the '288 and '416 patents, the "hardware key" or "access key" is an external hardware device that the account holder has in his or her physical possession and then connects to a personal computer:

> **The access key 450 is an external hardware device,** such as the iKey 1000 USB Smart Token device manufactured by Rainbow Technologies of Irvine, Calif. **The hardware token access device 450 preferably connects to the USB port of the account holder's personal computer. The major function of the hardware token access device 450 is to uniquely identify a account holder that desires to access the transaction services and computer resources of an untrusted network** such as the Internet. It is used in conjunction with the user name, password, and/or PIN to provide **two factor authentication**.

(Ex. A at 19:33-44[2]; *see also* Ex. B at 21:39-49.) To achieve two-factor authentication, users must *know* their username/password and *physically possess* their external hardware/access key with its unique digital identification, which allows them access to protected materials stored on a remote server. (*See, e.g.,* Ex. A at 19:44-47; Ex. B at 21:49-53.)

The '288 and '416 patent specifications state that a hardware key / access key is assigned to a user when he or she creates an account, and that the key contains a unique "digital identification" that identifies the user: "If the subscription uses two-factor authentication, the

[2] All emphasis is added unless otherwise noted.

approval process also involves assigning a unique digital ID to the applicant, and microcoding that digital ID inside an access key 54." (Ex. B at 14:50-53; *see also* Ex. A at 14:28-31.)

III. PROCEDURAL BACKGROUND

A. Delaware Litigation

On April 11, 2005, Prism filed suit in the District of Delaware alleging infringement of the '416 parent patent. *See Prism Techs. LLC v. Verisign, Inc. et al.*, Case No. 05-CV-00214-JJF (D. Del. 2005). In its claim construction brief, Prism affirmatively stated that "'[h]ardware key' is used synonymously with the terms 'access key' and 'hardware access key' in the specification. These terms therefore have the same meaning. The hardware key must be connected to the subscriber client computer such that 'the access key interface **reads the digital ID from the access key**.'" (Ex. C at 27-28 (citations omitted).) Prism went on to emphasize that this is a critical feature of its invention: **"The key point is that the subscriber client computer be able to <u>read</u> the 'predetermined digital identification' generated by the hardware key** … ." (*Id.* at 28.)

Prism argued to the Delaware court that the "hardware key" did not have to be external to the computer, but instead could be built into the device. Prism further argued that only "data," rather than a "predetermined digital ID," needed to be read from the key. (*See id.* at 27 ("**device or object from which <u>data</u> may be read <u>or emitted</u>**").) The Delaware court (Judge Farnan) rejected Prism's arguments. (*See* Exs. D & E.) The court explained:

> **[T]he specification requires that the hardware key be an external hardware device.** The Court declines to adopt Plaintiff's proposal that the key can be built into the computer, because **"the major function of the hardware key is to uniquely identify a user,"** and the specification teaches that the key should be something "which is known to have been assigned and given to a specific person." A hardware key built in to a computer is computer-specific, not user-specific.

(Ex. D at 18-19 (citations omitted).) Accordingly, the Delaware court construed "hardware key" to mean **"an external hardware device or object from which <u>the predetermined digital identification can be read</u>."** (Ex. E at 2.)

After the ruling, the parties stipulated there was no infringement under the court's claim construction. (*See* Ex. F.) Prism then appealed the claim construction order to the Federal Circuit. (*See* Ex. G.) In its appeal, Prism did not challenge the Delaware court's construction of "hardware key." (*Id.*) Prism did, however, challenge the construction of "connected," arguing that the hardware key could be built into the client computer:

> [N]othing in the actual claims of the '416 patent precludes "connected" from meaning "built in." …
>
> The hardware key stores user credentials, regardless of whether that key is external or built in. As long as the hardware key transmits the necessary digital identification, it will suffice.

(Ex. H at *32-37.)

The Federal Circuit rejected Prism's arguments and affirmed the Delaware court's constructions *per curiam*. *See Prism Techs. LLC v. Verisign, Inc.*, 263 Fed. Appx. 878 (Fed. Cir. 2008).

B. Nebraska Litigation Against RIM

On December 29, 2008, Prism filed suit in this Court, asserting infringement of the '288 patent. *See Prism Techs. LLC v. Research in Motion, Ltd. et al.*, Case No. 08-CV-537 (D. Neb. 2008). In its claim construction briefs, Prism once again argued that "'access key' is synonymous with 'hardware key.'" (*See, e.g.,* Ex. I at 14; Ex. J at 19 ("Both Prism and RIM agree that the terms 'hardware key' and 'access key' should each be construed the same").) Moreover, Prism repeatedly urged this Court to adopt the Delaware court's constructions for terms that were already construed, for example:

> Prism requests that the Court adopt the previous constructions for the terms as determined by the Delaware Court, as **those constructions are equally applicable to the claims of both the ’416 and the ’288 patent-in-suit**. (Ex. I at 6.)
>
> This Court need not repeat the efforts of the District Court in Delaware. (*Id*. at 10.)
>
> [The Delaware] decision is highly relevant to the claim terms at issue here because **the Patent Office considered the Delaware Court’s claim construction during the prosecution of the ’288 patent-in-suit**. (*Id*. at 11.)
>
> **Prism proposes that the common terms of the ’288 and ’416 patents be given the same construction.** The Federal Circuit has mandated that common claim terms of a parent and continuation-in-part application generally must be construed consistently. (*Id*. at 12.)
>
> The ’288 patent shares certain common claim terms with its parent ’416 patent. Those common claim terms should be construed similarly between the ’288 and the ’416 patents. (Ex. J at 11-13.)

Tellingly, at the same time it was proclaiming allegiance to the Delaware court’s constructions in the RIM case, Prism was in fact proposing the same incorrect modifications it is now pursuing in this case. (Ex. I at 14.) Prism settled the RIM case in May 2010, before the Court had a chance to rule on claim construction. It filed the instant litigation shortly thereafter, on June 8, 2010.

IV. THE ’288 PATENT CLAIMS AND PROSECUTION HISTORY

A. Overview of the Relevant Disclosure

The ’288 patent issued on October 30, 2007. (Ex. A.) It is entitled “Method and System for Controlling Access, by an Authentication Server, to Protected Computer Resources Provided via an Internet Protocol Network.” (*Id.*)

The ’288 patent describes a secure transaction system wherein hardware keys, each with a “unique embedded digital identification,” are distributed to users who connect them to their computers. (*See, e.g.,* Ex. A at 1:52-2:13.) The system includes four main components, depicted in the figure below: (1) a client computer device (shown in pink), (2) a hardware/access key associated with an account holder (shown in orange), (3) an access server (shown in purple), and (4) an authentication server (shown in green).

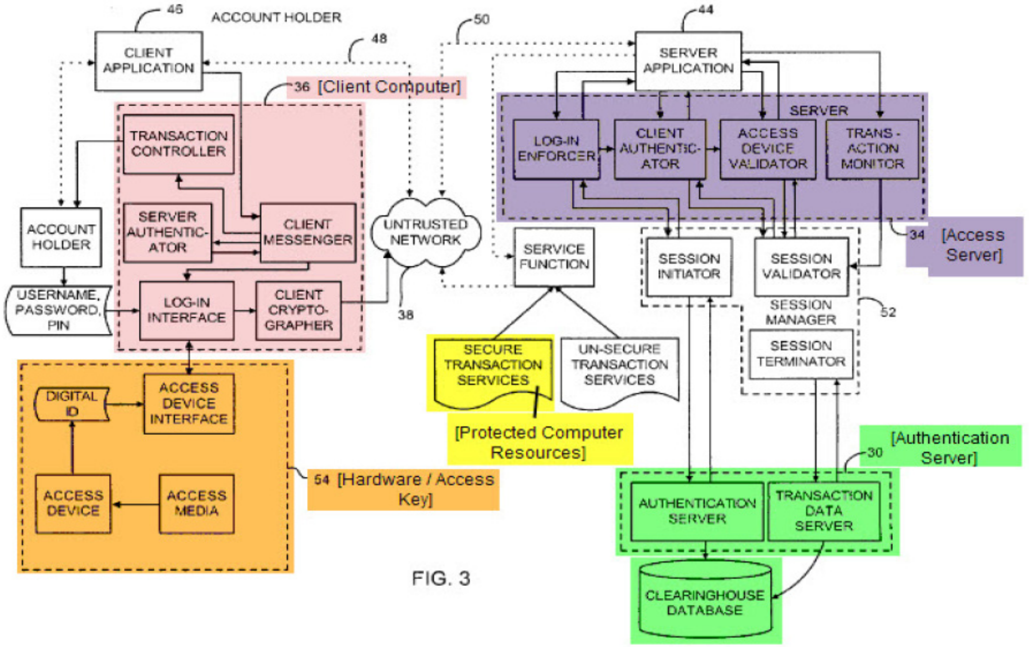

FIG. 3

(*Id*. at Fig. 3 (marked up by Prism in Ex. I at 3).)

When a user requests access to secure transaction services (i.e., protected computer resources) (shown in yellow) provided by the access server, the server prompts the user to enter "a username, a password, and/or a PIN[.]" (Ex. A at 16:15-18, 58-60.) Once this information has been entered, the client computer polls the hardware key interface (e.g., a USB port) for a connected hardware key. (*Id*. at 16:61-64.) If one is present, the hardware key interface reads the unique digital identification stored thereon. (*Id*. at 16:64-67.) The client computer then sends the login parameters, including the digital identification, to the access server. (*Id*. at 17:2-6.) The access server in turn sends an authentication request to the authentication server. (*Id*. at 17:9-12.)

The authentication server "accesses the account holder's information from its database and authenticates the login parameters," including comparing the digital identification received from the client to the account holder's digital identification stored in the database. (*Id.* at 17:12-18 ("If using two or three factor authentication, this authentication involves the comparison of the digital ID…").) The authentication server informs the access server whether the user has been authenticated or not. (*Id.* at 17:18-21, 31-34.) If authentication is successful, the access server may grant permission for the user to access the requested secure transaction services. (*Id.* at 17:27-31.) If unsuccessful, the access server denies permission to those services. (*Id.* at 17:36-38.)

The '288 patent added the concept of having the "hardware key" (designated throughout the patent by reference numeral 54) consist of two components – an "access device" and an "access media." (*See, e.g.,* Ex. A at Figs. 21-22; *see also id.* at 20:29-32 ("a magnetic card reader *access device* in use with an *access media* is implemented as the *hardware key*").) As shown in orange in Figure 3 (as annotated by Prism), these two terms are used in the '288 patent in reference to the hardware/access key. The "access media" stores the unique digital identification, and the "access device" reads the digital identification off the "access media" to provide it to the client computer via an "access device interface." (*See, e.g., id.* at Figs. 21-22; 7:49-53 ("the digital ID generated by the access media read by the hardware key attached to the account holder's computer").) For example, the '288 patent says that a "smart card reader access device in use with an access media is implemented as the hardware key 54." (*Id.* at 21:7-11.) The associated

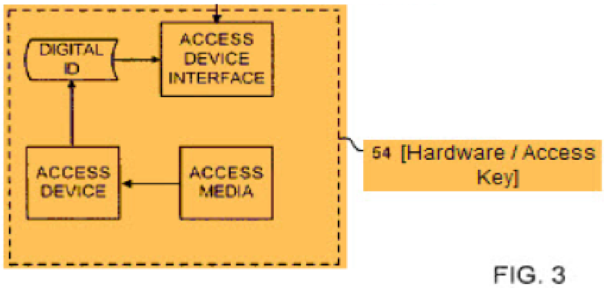

FIG. 3

figure (Fig. 23) shows that the "Smart Card" (containing the digital identification, labeled with the number "503") is the "Access Media" and the Smart Card Reader (labeled with the number "504") is the "Access Device." The "Hardware Key" (labeled with the number "54") is shown as a dotted line that includes both the Smart Card and the Smart Card Reader. (*Id.* at Fig. 23.)

B. Claims

The '288 patent includes a total of 187 claims, all of which require either a "hardware key" (claims 1, 31, 62, 87 and 116) or an "access key" (claims 117, 150, 186 and 187).[3] Claim 187 is exemplary:

> 187. A system for controlling access to protected computer resources provided via an Internet Protocol network, the system comprising:
>
> [a] **at least one authentication server having *an associated database to store (i) a digital identification associated with at least one client computer device*** requesting access to said protected computer resources, and (ii) data associated with said protected computer resources;
>
> [b] **said at least one client computer device having an associated <u>access key</u>, *said digital identification* being derived from said access key**;
>
> [c] said at least one client computer device adapted to forward ***said digital identification*** to at least one access server;
>
> [d] said at least one access server adapted to forward, to said at least one authentication server, ***said digital identification*** received from said at least one client computer device;
>
> [e] said at least one authentication server adapted to authenticate ***said digital identification*** responsive to a request for said protected computer resources by said at least once client computer device;

[3] The nine claims listed in this paragraph are the "independent" claims. The remaining 178 claims are "dependent," meaning they incorporate all of the requirements of the independent claim from which they depend.

[f] said at least one authentication server adapted to authorize said at least one client computer device to receive at least a portion of said requested protected computer resources, based on said stored data associated with said requested protected computer resources; and

[g] said at least one authentication server adapted to permit access to said at least said portion of said requested protected computer resources ***upon successfully authenticating said digital identification*** and upon successfully authorizing said at least once client computer device.

C. The Patent File Histories

In addition to the claim language itself, the patent file histories show the central importance of the external hardware/access key to Prism's claimed invention.

1. The '416 Patent

During prosecution of the '416 patent, the Examiner rejected Prism's claims in view of the prior art Stefik patent. Prism added the "hardware key" limitation to overcome that rejection. (*See* Ex. K at 1-5.) When the claims were allowed, the Examiner stated that the reason for allowance was the presence of the hardware key limitation:

> The closest prior art, Stefik (US 5,629,980) shows a system for controlling access to digital materials over a network by using a usage rights criteria for each subscriber or buyer. ***However, Stefik fails to disclose "the server requesting digital identification information from the client during an operating session and using the information to confirm that the hardware key associated with the client computer is connected*** to the subscriber's client computer." This distinct feature has been added to independent claims 1 and 28 and renders them allowable.

(Ex. L at 5.)

2. The '288 Patent

During prosecution of the '288 patent, Prism again used the hardware key feature to overcome various rejections of the claims in view of the prior art. (*See* Ex. M at 20-22

("Applicant submits that neither Tabuki nor Ault, either alone or in proper combination, teach or suggest the invention … ***at least due to the hardware key recitations in the claims*** as identified above").)

In 2007, while claim construction in the Delaware litigation was ongoing, the '288 patent was still under examination in the PTO. Just before Judge Farnan issued his claim construction ruling, Prism attempted to add new claims that omitted any "hardware key" or "access key" requirement. (*See* Ex. N at 23-35.) The Examiner, however, refused to allow Prism to expand its claims. By Examiner's Amendment, the PTO added the term "access key" back into the new claims and conditioned allowance of the '288 patent on Prism's acceptance of the Amendment. (Ex. O at 2-7.)

Significantly, during prosecution of the '288 patent, Prism notified the PTO of the Delaware court's claim constructions, making it part of the public record for the '288 patent. (Ex. P at 2.) Prism acknowledged the significance of this disclosure to this Court in the RIM litigation:

> Prism provided a copy of the Delaware Court's Memorandum and Opinion (construing the common claim terms identified here) to the Patent Examiner who prosecuted the '288 patent, thus, making it part of the intrinsic record. *IP Innovations LLC*, 2009 U.S. Dist. LEXIS at *6-7 ("Thus, in regard to the instant claim constructions, the court must take into consideration the prior constructions made in *Sony* and *Lexmark*. In addition, even if such prior rulings concerning the '780 Patent family were not presumptively binding in this case, the rulings would form part of the prosecution history and the intrinsic record for the court's primary consideration."). . . .

(Ex. I at 11-12.)

V. LEGAL STANDARDS

In interpreting patent claim terms, the question is how one of ordinary skill in the art would have understood those terms at the time of the filing of the patent. *See Phillips v. AWH Corp.*, 415 F.3d 1303, 1313 (Fed. Cir. 2005) (en banc). The starting point is the claims themselves, which define the boundaries of the invention. *See Vitronics Corp. v. Conceptronic, Inc*., 90 F.3d 1576, 1582 (Fed. Cir. 1996). The patent claims are interpreted with reference to the intrinsic evidence of the patents-in-suit, which includes the specification and prosecution history. *Phillips*, 415 F.3d at 1313 (*quoting Multiform Desiccants, Inc. v. Medzam Ltd*., 133 F.3d 1473, 1477 (Fed. Cir. 1998)). "[T]he specification 'is always highly relevant to the claim construction analysis. Usually, it is dispositive; it is the single best guide to the meaning of a disputed term.'" 415 F.3d at 1315. Courts may also examine extrinsic evidence if it is considered in the context of the intrinsic evidence and "the court deems it helpful in determining 'the true meaning of language used in the patent claims,'" but it is "less significant than the intrinsic record in determining 'the legally operative meaning of claim language.'" *Id*. at 1317-19 (*quoting Markman v. Westview Instruments, Inc*., 52 F.3d 967, 980 (Fed. Cir. 1995)).

The intrinsic evidence may reveal that the applicant disclaimed subject matter, distinguished prior art, disclaimed a potential claim interpretation, or otherwise limited the claims. *See Day Int'l, Inc. v. Reeves Bros. Inc*., 260 F.3d 1343, 1348 (Fed. Cir. 2001); *Chimie v. PPG Indus*., 402 F.3d 1371, 1384 (Fed. Cir. 2005). Where the intrinsic evidence reveals a disclaimer, or disavowal, of claim scope by the inventor, such revealed intention is dispositive. *See Honeywell Int'l. Inc. v. ITT Indus., Inc*., 452 F.3d 1312, 1319-20 (Fed. Cir. 2006).

The Court must consider not only the specification and prosecution history of the patent-in-suit, but also the specification and prosecution history of any parent patents, in order to understand common claim terms. *See Microsoft*, 357 F.3d at 1350 ("Any statement of the patentee in the prosecution of a related application as to the scope of the invention [is] relevant to claim construction"); *Jonsson v. Stanley Works*, 903 F.2d 812, 818 (Fed. Cir. 1990).

VI. ARGUMENT

A. "Hardware Key" and "Access Key" Proposed Constructions

Delaware Construction	Defendants' Proposed Construction	Prism's Proposed Construction
an external hardware device or object from which **the predetermined** digital identification can be **read**	An external hardware device or object from which **the predetermined** digital identification can be **read**	external hardware device or object from which **a** digital identification can be **generated, derived or read**

Plaintiff and Defendants agree that the terms "access key" and "hardware key" mean the same thing, and that they describe an external hardware device. The only disputes between the parties with respect to these terms are (1) whether the digital identification must be ***read*** from the hardware key; and (2) whether it is ***the predetermined digital identification*** that must be read, or some other unspecified "digital identification."

B. The Digital Identification Must be *Read* from the Hardware Key to Authenticate an Account Holder

1. "Reading" the digital identification from the hardware key is required

The specification of the '288 patent clearly, and repeatedly, states that, in every instance, the digital identification must be *read* from the hardware key to authenticate an account holder. For example, the patent states that when using two-factor authentication, "the hardware key interface **reads** the digital ID from the access media[4] and sends it to the login interface (block 146)." (Ex. A at 16:64-67.) The associated figure (Figure 16) illustrates the log-in process, and states that the "access device interface **reads** the digital ID from access device and sends it to log-in interface." (*Id*. at Fig 16.) This aspect of the invention is repeated throughout the

[4] As noted above, and as shown in the various figures in the '288 patent, the "access media" is the part of the hardware key that stores the digital identification.

specification as an essential feature of the hardware key. (*See e.g. id.* at 13:37-39 ("…the account holder software 36 polls the hardware key 54, [and] **reads** the digital ID from the access media…"); *id.* at 18:33-40 ("The access device interface polls the account holder's machine for the hardware key 54 and **reads the digital ID** from the access media. If the digital ID is successfully **read**, the program implements a session renewal, which is shown in FIG. 19. If the digital ID is not successfully **read**, the access device interface sends an error message to the login interface…"); *id.* at 18:47-49 ("the access device interface **reads the digital ID** of the access media and submits it to the login interface…").)

Reading the digital identification from the hardware key is required because, in the invention of the '288 patent, that is where the digital identification is actually *stored.* All hardware key embodiments in the '288 patent store the digital identification such that it is read from the hardware key. For example, the '288 patent describes using an "iKey 1000 USB Smart Token device" (shown at right) as an access key. This device includes a memory that stores "information for personally identifying the account holder," and the computer reads the digital identification from that memory using the computer's USB port. (*See id.* at 19:30-20:28 and Fig. 21.)

The magnetic card example stores the digital identification on a strip of magnetic recording tape, and the client computer reads the digital identification using a magnetic card reader attached to the user's computer. (*Id.* at 20:29-21:6 and Fig. 22.) Similarly, the smart card embodiment is embedded with a computer chip that "can contain several digital IDs" that are read by a "Smart Card reader" attached to the user's computer. (*Id.* at 21:7-54 and Fig. 23.) A "biometric identification reader access device" can obtain biometric data by using a fingerprint or retina scanner, convert that unique fingerprint into a digital identification and store it in a "local repository" on the reader. (*Id*. at 21:55-22:29 and Fig. 24.) In all of these embodiments, regardless of how the digital identification is created, it is stored within the hardware key itself, so that client computer can read that digital identification when the hardware key is connected to the computer.

Prism itself emphasized this exact point in Delaware, arguing that "The key point is that the subscriber client computer be able to *read* the 'predetermined digital identification' generated by the hardware key" and "[t]he hardware key must be connected to the subscriber client computer such that the access key interface *reads* the digital ID from the access key." (Ex. C at 28.)

The Delaware court agreed, construing "hardware key" to mean external hardware ***"from which the predetermined digital identification can be <u>read</u>."*** (Ex. E at 2.) The Delaware court arrived at this construction even though some claims of the '416 patent, like the '288 patent, additionally required the hardware key to "generate" the predetermined digital identification. (*See, e.g.,* Ex. B at 35:46-49.) As set forth above, Prism chose not to challenge the Delaware construction of "hardware key." (*See* Ex. G.)

Prism admits that the Delaware court's construction "is highly relevant to the claim terms at issue here because the Patent Office considered the Delaware Court's claim construction during the prosecution of the '288 patent-in-suit." (Ex. I at 11.) Indeed, according to Prism, it explicitly "informed the Patent Examiner that … certain common terms had been construed by the District Court of Delaware" and "provided a copy of the Delaware Court's Memorandum and Opinion (construing the common claim terms identified here) to the Patent Examiner who prosecuted the '288 patent, thus, making it part of the intrinsic record." (*Id.*) Thus, Prism made every effort to have the Examiner analyze the patentability of the claims of the ’288 patent under the Delaware court’s construction. (*See id*. (“the Patent Examiner for the ’288 patent acknowledged that he considered the Order construing the claims of the parent ’416 patent”).) Having done so, Prism cannot now argue its claims are broader for determining infringement than they were for determining patentability.

2. Prism’s proposed construction improperly makes “reading” the digital identification from the hardware key optional

While Prism purported to embrace the Delaware court’s construction in its earlier briefing to this Court, it actually proposes here (as it did in the RIM case) a different construction of hardware key that improperly deviates from the Delaware court’s construction. The Delaware court’s construction says the hardware key is an external hardware device **“from which the predetermined digital identification is read,”** but Prism proposes modifying that construction to say **“from which a digital identification is *generated, derived or read*.”**

Prism’s proposal removes a key structural feature of the hardware key from the claims. By using the word “or,” Prism’s proposed construction would make reading the digital identification an optional feature of the hardware key, contrary to the express teachings of the specification and the hardware key’s essential function. By requiring only that the digital identification can be “generated, derived ***or*** read,” Prism suggests that in some instances the digital identification can be generated or derived from, but not actually read from, the hardware key itself. However, as discussed above, in every instance the specification teaches that the digital identification is read from the hardware key, not from any other source. Without this step, authentication cannot take place.

The reason Prism makes this argument is clear – it knows Defendants do not provide an external hardware key with their software. It knows there is no digital identification read from identical copies of installation CDs. So Prism seeks to broaden the construction of hardware key, presumably to try and point to some unspecified digital identifier stored somewhere else in the system. By adding "generated" and "derived" as alternatives to "read," Prism likely intends to suggest that reading the digital identification from the hardware key is optional, thereby depriving the hardware key of its essential function in the '288 patent – to uniquely identify a user. There is no support in the patent for such a construction, and the Court should not allow Prism to broaden its alleged invention in this manner.

3. Certain claims include the additional requirement that the hardware key "generate a digital identification"

Separate from the requirement that the hardware key be "an external hardware device or object from which the digital identification can be read," certain claims of the '288 patent contain the additional requirement that the hardware key also perform the *additional* step of "generating" the digital identification. For example, claim 1 of the '288 patent states that there is "at least one hardware key associated with said at least one client computer device, **said at least one hardware key generating a digital identification**…" (Ex. A at 35:7-9.)

The fact that certain claims expressly require the hardware key to "generate" a digital identification provides further support that Prism's proposed construction is wrong. Generating the digital identification is not an optional part of these claims. Also, the hardware key is not something "**from which**" the digital identification can be generated by some other, unnamed component. To the contrary, in those embodiments, the hardware key *itself* generates and stores the digital identification. (*See, e.g.*, *id*. at 1:62-63 ("the [hardware] key being adapted **to generate** a digital identification as part of the digital data").) Because the hardware key is an *external* hardware device, the only way the client computer can get that digital identification after it has been generated is to read it from the hardware key.

The Delaware court's construction for "hardware key" further supports the conclusion that the "hardware key" must be something from which the digital signature can be read. Like the '288 patent, the '416 patent includes claims that additionally require the hardware key to "generate a predetermined digital identification." (*Compare* Ex. A at 35:8-9 ('288 patent, claim 1 – "said at least one hardware key generating a digital identification") with Ex. B at 35:46-48 ('416 patent, claim 1 – "said [hardware] key being adapted to generate a predetermined digital identification").) This parallelism between the claim language in the two patents, and the Delaware court's construction, demonstrates that inclusion of the term "generate" in certain claims does not support Prism's argument that reading the digital identification from the hardware key is optional, or that the claim language of the '288 patent merits a departure from the Delaware court's construction.

4. The word "derived" does not appear anywhere in the patent specification, and Prism has refused to clarify what it means

The independent claims of the '288 patent that contain the "access key" limitation (i.e., claims 117, 150, 185, 186 and 187) all say that the digital identification is "derived" from the access key. (*See, e.g.,* Ex. A at 45:12-13.) However, the word "derived" does not appear anywhere in the specifications of either the '288 patent or the '416 patent. Thus, adding it to the construction of "access key" would itself require further construction.

On January 14, 2011, in an effort to narrow the dispute and understand Prism's proposed construction, Defendants asked Prism to explain how the term "derived" differs from the terms "read" or "generated." (*See* Ex. Q ("Does Prism believe the word 'derived' has a meaning different from 'read' or 'generated,' and if so, can you clarify that distinction and what Prism believes the word 'derived' means?").) On January 24, ten days later and just four days before this brief was due, Prism responded and refused to provide an explanation, saying it was declining to "construe its construction…" (Ex. R.) This highlights the central problem with Prism's proposal – it improperly seeks to interject ambiguity where none exists.

In the RIM litigation, Prism similarly attempted to avoid the question of what the term "derived" means. However, it did state that "to the extent the Court believes the term requires additional construction for the jury, Prism proposes 'obtaining ***or reading.***'" (Ex. J at 23.) Prism did not explain how "obtaining" differs from "reading." Nevertheless, Prism's statement acknowledges that the ordinary meaning of "derived" is synonymous with "read." The written description of the '288 patent overwhelmingly supports this conclusion because, as set forth above, the '288 patent consistently describes reading the digital identification from the hardware key to perform two-factor authentication. To the extent "derived" means the same thing as "read," there is no reason to include it in the claim construction because it is redundant. To the extent it means anything broader than "read," it is unsupported by the specification. Either way, there is no reason to interject ambiguity into the construction by adding the term "derived."

As discussed above, Prism knows Defendants do not provide a hardware key with their products, and do not store any sort of unique digital identification on their installation CDs. Thus, the only way that Prism can hope to argue that the hardware key requirement is met is to try and broaden its claims using this ambiguity. It does so by suggesting "derived" means something *different* than "read" – suggesting that a digital identification stored elsewhere in the system can meet the claims, and that the digital identification does not have to be read from the hardware key itself. The purpose of claim construction, however, is to clarify terms, not to inject new ambiguity. *See O2 Micro Int'l Ltd. v. Beyond Innovation Tech. Co.*, 521 F.3d 1351, 1360-61 (Fed. Cir. 2008) ("The purpose of claim construction is to determine the meaning and scope of the patent claims asserted to be infringed"). Accordingly, the Court should reject Prism's proposal and instead adopt the Delaware court's construction verbatim.

C. It Is "The Predetermined Digital Identification" That Must Be Read from the Hardware Key

The second way in which Prism proposes to alter the Delaware court's construction is to modify what is actually read from the hardware key. Specifically, Prism attempts to broaden the construction by changing what is read from the hardware key from "**the predetermined** digital identification" to merely "**a** digital identification**.**" As noted, it appears that Prism is attempting to point to a digital identification of some kind stored outside the hardware key. Doing so, however, violates basic canons of claim construction requiring that terms be read in the context of both the specification and the claims of which they are a part. *See Phillips*, 415 F.3d at 1314 ("the claims themselves provide substantial guidance as to the meaning of particular claim terms"). Surrounding claim language can add context to the meaning of a term, and here it does just that.

All of the claims of the '288 patent require that the authentication server use the digital identification to "authenticate" the client computer. As shown in exemplary claim 187, above, all claims require pre-storing a digital identification in a database associated with the authentication server. (*See, e.g.,* Ex. A at 51:4-7 and 52:1-4 (claim 187) – "at least one authentication server having **an associated database to store (i) a digital identification associated with at least one client computer device** requesting access to said protected computer resources … said at least one authentication server adapted to authenticate said digital identification responsive to a request … by said … client computer device….")

In order for two-factor authentication to work, the authentication server must compare the digital identification that is read from hardware key and sent from the client computer with the predetermined digital identification that is stored in the database associated with the authentication server. (*See, e.g.,* Ex. A at 12:17-20 ("The session manger [sic] 52 authenticates the digital ID **by comparing it to the information it has** in the session entry for the particular account holder"); *see also id.* at 17:12-18 ("…the account holder authentication server accesses the account holder's information from its database and authenticates the login parameters. If using two or three factor authentication, **this authentication involves the comparison of the digital ID**…"); *id.* at 22:20-22 ("The digital ID created by the biometric data would be **compared to the digital ID already stored in the transaction clearinghouse** for authenticity…").) If the authentication server did not know the digital identification before it was sent (i.e., if it was not "predetermined"), there would be no way for it to authenticate the user, as all the claims require.

Moreover, when a claim term is preceded by the articles "the" or "said," it is construed to refer back to the earlier instance of that term in the claim. *See, e.g., Process Control Corp. v. HydReclaim Corp.,* 190 F.3d 1350, 1356 (Fed. Cir. 1999) ("The presence of that identical language clearly indicates that 'a discharge rate' in clause [b] is the same as 'the discharge rate' in clause [d]"). Accordingly, "said" digital identification in claim 187, and the corresponding language in the other claims, necessarily refer back to the same digital identification stored in the database and used to authenticate the account holder – i.e., it is "predetermined."

The Delaware court's construction properly recognizes the surrounding claim language and the role of the hardware key in the invention, and correctly requires that "the predetermined digital identification" be read from the hardware key, as opposed to just "a digital identification." Prism has no basis for contending that this requirement should be jettisoned in this case.

VII. CONCLUSION

For all of the foregoing reasons, the Court should adopt the Delaware court's construction and construe both "hardware key" and "access key" as **"an external hardware device or object from which the predetermined digital identification can be read."**

Dated: January 28, 2011

Respectfully submitted,

/s/ Kelly C. Hunsaker
Frank E. Scherkenbach (admitted pro hac vice)
FISH & RICHARDSON P.C.
225 Franklin Street
Boston, MA 02110
Telephone: (617) 542-5070
Facsimile: (617) 542-8906
scherkenbach@fr.com

Kelly C. Hunsaker (admitted pro hac vice)
Jonathan J. Lamberson (admitted pro hac vice)
FISH & RICHARDSON P.C.
500 Arguello Street, Suite 500
Redwood City, CA 94063
Telephone: (650) 839-5070
Facsimile: (650) 839-5071
hunsaker@fr.com
lamberson@fr.com

L. Steven Grasz (SBN 19050)
Michael S. Degan (SBN 20372)
Michael T. Hilgers (pro hac vice)
HUSCH BLACKWELL LLP
1620 Dodge Street, Suite 2100
Omaha, NE 68102
Telephone: (402) 964-5000
Facsimile: (402) 964-5050
steve.grasz@huschblackwell.com
mike.degan@huschblackwell.com
michael.hilgers@huschblackwell.com

Attorneys for Defendants
ADOBE SYSTEMS INCORPORATED AND
NATIONAL INSTRUMENTS
CORPORATION

/s/ Rudy Y. Kim
Rudy Y. Kim (pro hac vice)
Erika L. Yawger (pro hac vice)
MORRISON & FOERSTER LLP
755 Page Mill Road
Palo Alto, California 94304
Telephone: (650) 813-5600
Facsimile: (650) 494-0792
rudykim@mofo.com
eyawger@mofo.com

Michael A. Jacobs (pro hac vice)
MORRISON & FOERSTER LLP
425 Market Street
San Francisco, California 94105
Telephone: (415) 268-7000
Facsimile: (415) 268-7522
mjacobs@mofo.com

John P. Passarelli (SBN 16018)
KUTAK ROCK LLP
The Omaha Building
1650 Farnam Street
Omaha, Nebraska 68102
Telephone: (402) 346-6000
Facsimile: (402) 346-1148
john.passarelli@kutakrock.com

Attorneys for Defendants
AUTODESK, INC.

/s/ Ruben S. Bains
Danny L. Williams (pro hac vice)
Ruben S. Bains (pro hac vice)
Matthew R. Rodgers (pro hac vice)
WILLIAMS, MORGAN & AMERSON, P.C.
10333 Richmond Avenue, Suite 1100
Houston, Texas 77042
Telephone: (713) 934-7000
Facsimile: (713) 934-7011
dwilliams@wmalaw.com
rbains@wmalaw.com
mrodgers@wmalaw.com

Attorneys for Defendants
MCAFEE, INC. and THE MATHWORKS, INC.

/s/ Scott W. Breedlove
Scott Breedlove (pro hac vice)
Giriraj Pathmanaban (pro hac vice)
VINSON & ELKINS LLP
2001 Ross Ave. – Suite 3700
Dallas, TX 75201
Telephone: (214) 220-7700
Facsimile: (214) 220-7716
sbreedlove@velaw.com
gpathmanaban@velaw.com

Richard P. Jeffries, #20089
CLINE WILLIAMS WRIGHT,
JOHNSON & OLDFATHER, L.L.P.
One Pacific Place
1125 South 103rd Street, Suite 320
Omaha, Nebraska 68124
Telephone: (402) 397-1700
Facsimile: (402) 397-1806
rickjeffries@clinewilliams.com

Attorneys for Defendants
NUANCE, INC.

/s/ Jonathan Singer
L. Steven Grasz (SBN 19050)
Michael S. Degan (SBN 20372)
Michael T. Hilgers (pro hac vice)
HUSCH BLACKWELL LLP
1620 Dodge Street, Suite 2100
Omaha, NE 68102
Telephone: (402) 964-5000
Facsimile: (402) 964-5050
steve.grasz@huschblackwell.com
mike.degan@huschblackwell.com
michael.hilgers@huschblackwell.com

Jonathan Singer (pro hac vice)
FISH & RICHARDSON PC
60 South 6th Street, Suite 3200
Minneapolis, MN 55402
Telephone: (612) 335-5070
Facsimile : (612) 288-9696
singer@fr.com

Lara S. Garner (pro hac vice)
FISH & RICHARDSON PC
12390 El Camino Real
San Diego, CA 92130
Telephone: (858) 678-4332
Facsimile: (858) 678-5070
lgarner@fr.com

Attorneys for Defendants
SAGE SOFTWARE, INC.

/s/ Dean G. Dunlavey
Mark A. Flagel (pro hac vice)
Dale Chang (pro hac vice)
LATHAM & WATKINS LLP
355 South Grand Avenue
Los Angeles, California 90071-1560
Telephone: (213) 485-1234
Facsimile: (213) 891-8763
mark.flagel@lw.com
dale.chang@lw.com

Dean G. Dunlavey (pro hac vice)
LATHAM & WATKINS LLP
650 Town Center Drive, 20th Floor
Costa Mesa, California 92626-1925
Telephone: (714) 755-8260
Facsimile: (714) 755-8290
dean.dunlavey@lw.com

Richard P. Jeffries (SBN 20089)
CLINE WILLIAMS WRIGHT
JOHNSON & OLDFATHER, L.L.P.
One Pacific Place
1125 South 103rd Street - Suite 320
Omaha, Nebraska 68124
Telephone: (402) 397-1700
Facsimile: (402) 397-1806
rickjeffries@clinewilliams.com

Attorneys for Defendant
SYMANTEC CORP.

/s/ Mark D. Fowler
L. Steven Grasz (SBN 19050)
Michael S. Degan (SBN 20372)
Michael T. Hilgers (pro hac vice)
HUSCH BLACKWELL LLP
1620 Dodge Street, Suite 2100
Omaha, NE 68102
Telephone: (402) 964-5000
Facsimile: (402) 964-5050
steve.grasz@huschblackwell.com
mike.degan@huschblackwell.com
michael.hilgers@huschblackwell.com

Mark D. Fowler (pro hac vice)
Robert Buergi (pro hac vice)
Marc C. Belloli (pro hac vice)
DLA Piper LLP (US)
2000 University Ave.
East Palo Alto, CA 94303-2214
Telephone: (650) 833-2000
Facsimile : (650) 833-2001
mark.fowler@dlapiper.com
robert.buergi@dlapiper.com
marc.belloli@dlapiper.com

Attorneys for Defendants
TREND MICRO INCORPORATED

CERTIFICATE OF SERVICE

The undersigned hereby certifies that a true and correct copy of the above and foregoing document has been served on January 28, 2011 to the following counsel of record via the Court's CM/ECF system:

Carmen M. Aviles
LANIER LAW FIRM
2200 Geng Rd., Ste. 200
Palo Alto, CA 94303
Email: cma@lanierlawfirm.com
Attorneys for Prism Technologies LLC

Daniel J. Fischer
KOLEY, JESSEN LAW FIRM
1125 South 103rd Street
Suite 800, One Pacific Place
Omaha, NE 68124
Email: dan.fischer@koleyjessen.com
Attorneys for Prism Technologies LLC

Dara G. Hegar
LANIER LAW FIRM
6810 FM 1960 West
Houston, TX 77069
Email: dgh@lanierlawfirm.com
Attorneys for Prism Technologies LLC

Michael C. Cox
KOLEY, JESSEN LAW FIRM
1125 South 103rd Street, Suite 800
Omaha, NE 68124
Email: mike.cox@koleyjessen.com
Attorneys for Prism Technologies LLC

André J. Bahou
PRISM TECHNOLOGIES, LLC
878 Arlington Heights Dr., Ste. 400
Brentwood, TN 37027
Email: aj.bahou@prismpatent.com
VP and Chief Intellectual Property Officer of Prism

Christopher D. Banys
LANIER LAW FIRM
2200 Geng Rd., Ste. 200
Palo Alto, CA 94303
Email: cdb@lanierlawfirm.com
Attorneys for Prism Technologies LLC

Daniel M. Shafer
LANIER LAW FIRM
2200 Geng Rd., Ste. 200
Palo Alto, CA 94303
Email: dms@lanierlawfirm.com
Attorneys for Prism Technologies LLC

James D. Tario
LANIER LAW FIRM
2200 Geng Rd., Suite 200
Palo Alto, CA 94303
Email: jdt@lanierlawfirm.com
Attorneys for Prism Technologies LLC

W. Mark Lanier
LANIER LAW FIRM
6810 FM 1960 West
Houston, TX 77069
Email: wml@lanierlawfirm.com
Attorneys for Prism Technologies LLC

David A. Yudelson
KOLEY JESSEN P.C., L.L.O.
1125 s. 103RD St., Ste. 800
Omaha, NE 68124
Email: David.Yudelson@koleyjessen.com
Attorneys for Prism Technologies LLC

Francine M.B. Lopacinski